

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

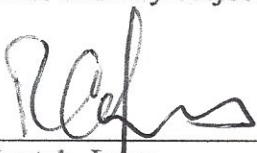
1. Date filed: February 21, 2018
2. Name of company covered by this certification: Lyons Communications, LLC.
3. Form 499 Filer ID: 830367
4. Name of signatory: Robert A. Jones
5. Title of signatory: President
6. Certification:

I, Robert A. Jones, certify that I am an officer of Lyons Communications, LLC ("Lyons"), and, acting as an agent of Lyons, that I have personal knowledge that Lyons has established operating procedures, as summarized in the attached statement, that are adequate to ensure compliance with the customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how Lyons' procedures ensure that it is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in Section 64.2001 *et seq.* of the Commission's rules.

Lyons has not received any customer complaints in the past calendar year or any prior year concerning unauthorized release of CPNI. Lyons has not taken any actions in the past year or any prior year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject Lyons to enforcement actions.

  
\_\_\_\_\_  
Robert A. Jones  
President  
Lyons Communications, LLC  
Executed February 21, 2018

## **CPNI Compliance Policies of Lyons Communications, LLC**

The following summary describes the policies of Lyons Communications, LLC ("Lyons") that are designed to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.* CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

These policies are managed by Lyons's CPNI Compliance Manager, Robert Jones.

### **I. USE, DISCLOSURE OF, AND ACCESS TO CPNI**

Lyons will use, disclose, or permit access to individually identifiable CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Lyons, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Lyons does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Although Lyons's current policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve the CPNI Compliance Manager. If such use is approved, Lyons shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

Lyons does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When Lyons receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

### **II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES**

Above and beyond the specific FCC requirements, Lyons will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to



obtain unauthorized access to CPNI, or of possible changes to Lyons's existing policies that would strengthen protection of CPNI, they should report such information immediately to the CPNI Compliance Manager so that Lyons may evaluate whether existing policies should be supplemented or changed.

**A. Online Accounts**

When customer initiates service, a random password is provided to their address of record. Because the password is randomly generated, it is not expected to include the customer's account or biographical information. Upon initial entry into the on-line portal through this link, the customer is provided an opportunity to create a new password and an email address to be used for password recovery. The website advises the customer to choose a strong password that does not include easily guessed information such as their name, telephone number, social security number, or account number. A password and password recovery email may thereafter be changed by the customer only after logging into the online account with the correct login ID and password. If a customer forgets their password and does not have access to the password recovery email, they may only obtain new credentials by contacting Lyons by phone and asking for these a new password to be provided by a return telephone call to the telephone number of record for the account, or sent to the address of record that has been on file for 30 days, or they may visit the Lyons office and present photo identification that meets the requirements of Section II.C. below.

**B. Inbound Calls to Lyons Requesting CPNI**

CSRs may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated.

More stringent protections apply to Call Detail Information (CDI), which includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. Even after a caller has been authenticated under the process above, Lyons does not reveal CDI to an inbound caller. Instead, if an inbound caller requests CDI, the CSR will first encourage them to obtain the information from their online account. If the caller is unable or not interested to obtain the information from their online account, Lyons may offer to provide the requested CDI by sending the information by mail to a mailing address of record for the account, but only if such address has been on file with Lyons for at least 30 days. Alternatively, a customer may obtain CDI at the Lyons office in accordance with Section II.C below.

**C. In-Person Disclosure of CPNI at the Lyons Office**

Lyons may disclose a customer's CPNI to an authorized person visiting the Lyons office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

#### **D. Notice of Account Changes**

Whenever a password or online account is created or changed, Lyons will provide a notice to a customer address of record. Whenever a postal or e-mail address of record is created or changed, Lyons will send a notice to customer's prior address of record notifying them of the change. The foregoing notifications are not required when the customer initiates service, including the selection of an email address or creation of an online account at service initiation. Each of the notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Lyons if they did not authorize the change.

### **III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT**

Any Lyons employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the CPNI Compliance Manager. Such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Lyons's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Lyons's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

#### **A. Identifying a "Breach"**

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a Lyons employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Lyons's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. The CPNI Compliance Manager will determine whether it is appropriate to update Lyons's CPNI policies or training materials in light of any new information; the FCC's rules require Lyons on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."



## **B. Notification Procedures**

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. Lyons's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450) for instructions.

Lyons will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below. (A full business day does not count a business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure.

If Lyons receives no response from law enforcement after the 7<sup>th</sup> full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Lyons will delay notification to customers or the public upon request of the FBI or USSS. If the CPNI Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Lyons still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

## **IV. RECORD RETENTION**

The CPNI Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Lyons maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Lyons later changes its policies to permit the use of CPNI for marketing, it will revise its recordkeeping policies to comply with the Commission's recordkeeping requirements.

Lyons maintains a record of all customer complaints related to their handling of CPNI, and records of Lyons's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that Lyons considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Lyons will have an authorized officer, as an agent of Lyons, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Lyons has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC by the first business day or on after March 1 of the

subsequent year, and will be accompanied by a summary or copy of this policy that explains how Lyons's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

## **V. TRAINING**

All employees with access to CPNI receive a copy of Lyons's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Lyons requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.